REMARKS

Claims 1-14 and 16-29 are pending in this application.

Claim Rejections Under 35 U.S.C. §103

Claims 1-14 and 16-29 were rejected under 35 U.S.C. §103 as being unpatentable over Reeds III (U.S. Patent No. 5,724,427) in view of Thornwall (U.S. Patent No. 4,675,477.

In the system invention as claimed herein, the encryption software includes an encryption substitution set, comprised of randomly-generated elements, and an encoding matrix which cross-multiplies the message elements, to generate the patternless encrypted message. The decrypting of any portion of the encrypted message does not provide a pattern for enabling generating a key to decrypt the entire message, since the encrypted message is patternless. Furthermore, the decrypting of any portion or all of the patternless encrypted message with a phony key generated by a third party from the patternless encrypted message generates false positives, which prevent the third party from determining the correct key and/or plain text message.

Reeds III, in contrast to the claimed invention, discloses a system for block or stream encrypting text using an autokeyed rotational state vector to encrypt plain text to yield cipher text. In Reeds III the same rotational state vector is applied to each byte of the plain text for encryption to yield a byte of cipher text, creating a pattern. Also, the

rotational state vector is updated or changed as a function of one or more of the cipher text, plain text, or key, creating a pattern. The use of a function creates a pattern in the encryption, whereby if a portion of the encrypted message is decrypted, the function utilized for the key is determinable, and the key and/or message are determinable, since the same function is repeated throughout by autokeying thereof. Also, the shift in the translation table is a single shift of elements and not a multiple shift, and the elements are not randomly generated set elements. Further, there is no disclosure or suggestion of an encoding matrix which cross-multiplies the message elements, and which, together with the randomly-generated set elements and multiple shiftkey replacement, generates the patternless encrypted messages, as in the claimed invention.

In Thornwall, contrary to the claimed invention, the device is an electronic version of an expanded lookup-table, with a single shift of elements, not a multiple shift, and the elements in the encryption substitution set are not randomly generated, but are instead selected from the same lookup-table, creating a pattern. Further, the message elements are not cross-multiplied in an encoding matrix. The device generates a very specific pattern from the lookup-table, and is not patternless (figure 1; column 1, lines 28-42; column 2, lines 32-49).

Therefore, there is no evidence in Reeds III and Thornwall of the configuration herein, since they do not teach or suggest the claimed invention.

Dependent Claims

In view of the patentability of the underlying independent claims over the references as set forth above, it is submitted that the claims depending therefrom are likewise patentable.

CONCLUSION

It is submitted in view of the above that there is no teaching or suggestion of applicant's invention as claimed herein, within the scope of the disclosure of the cited references, without extensive modification and the exercise of inventive talent.

In light of the above amendments and remarks, applicant submits that the application is in condition for allowance, and requests that it be passed to issue. If there are any issues which can be discussed in a telephone interview, the Examiner is requested to contact applicant's attorney at (310) 242-2732.

Respectfully submitted,

FULWIDER PATTON LLP

Date: April 9, 2008

By: /howard n. sommers/
Howard N. Sommers
Registration No. 24,318

Howard Hughes Center
6060 Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696

201176.1

Serial No.: 10/631,326
Client ID/Matter No.: MSKI-63168